

Technician and Philosopher

Building the Relevance and Intellectual Capital of the Army's Information Warriors

James E. Shircliffe, Jr.

James E. Shircliffe, Jr., is a program manager with the Federal Bureau of Investigation in Washington, DC. He has worked as an intelligence analyst for a variety of government agencies, to include the Department of Defense and the FBI. His areas of expertise include counterintelligence and technical operations analysis. Mr. Shircliffe earned a B.A. from the Virginia Military Institute and a M.S. from American Military University.

PHOTO: U.S. Air Force 1LT Georganne Hassell, the information operations officer of Provincial Reconstruction Team Zabul, looks out across the city during a presence patrol along the outskirts of Qalat City, Afghanistan, 23 July 2010. (DOD photo by Senior Airman Nathanael Callon, U.S. Air Force)

NUMEROUS CONVERSATIONS, PAPERS, books, and presentations stress the need for the Army to compete more effectively against a multitude of state and nonstate actors in the information environment. However, the Army often forgets that this competition does not take place between large, faceless organizations. It is a struggle of a group of professionals—information warriors—who must match wits with agile, thinking foes who do not always observe the same rules of engagement or moral strictures as U.S. forces. Talk about influencing the information environment is cheap, but is the Army ready to invest in a nontraditional educational regimen and a professionally rewarding career path for Information Operations (IO) officers?

The key to developing a strong information warrior cadre and culture is to create a broader Army organizational culture that values IO's contribution. The first step in this effort is to develop a group of information warriors of such capability and quality that they can demonstrate a mastery of their trade and explain what they can do for the commander, what assets they need, and then deliver. However, the IO field is not the easiest specialty in the Army, nor are its core capabilities easy to master. Information warrior education should include numerous training sabbaticals, in both hard and soft science fields, and opportunities for cultural and language immersion. In the field or in the corridors of the Pentagon, successful IO requires officers who can get IO recognized as a value-added tool worthy of the same recognition as artillery and close air support. This is a bureaucratic skill that we must identify and cultivate. It is often critical in making IO work, and it cannot be taught.

The Challenge

The information that people receive drives their cognition, and hence their action or inaction. If we can properly manipulate the information that a target population receives, then we can steer that population's actions in directions advantageous to national and operational objectives. A target population can be of any size: it can be a single individual, such as a

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE NOV 2010		2. REPORT TYPE		3. DATES COVERED 00-11-2010 to 00-12-2010	
4. TITLE AND SUBTITLE Technician and Philosopher: Building the Relevance and Intellectual Capital of the Army's Information Warriors				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Combined Arms Center, Military Review, Truesdell Hall, 290 Stimson Ave., Unit 2, Fort Leavenworth, KS, 66027				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 6	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

national leader, or a brigade staff, or the residents of a town or an entire nation.

More often than not, the goal of the commander is to target the decision making of an opposing commander and the morale of his soldiers. This is the purpose of maneuver, surprise, flanking, or even wearing the outlandish costumes of the barbarians who took on the armies of the Roman Republic. The movement of kinetic assets in relation to those of an opposing force, or their movement to a sensitive site (such as a nation's capital), can generate fear, alter the cost-benefit calculation, and lead to limited skirmishes. Altering the cost-benefit calculation forecloses an opponent's courses of action and can push him to take actions advantageous to friendly forces. "Shock and awe" is a more contemporary example of the use of military force to influence specific populations. Often, the point of maneuver warfare is not to attrit forces, but to exploit the opposition's psychology by presenting information in the form of force disposition.

Joint Publication 3-13 defines information operations:

The integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.¹

There are kinetic operations, and there is IO—all those other warfighting capabilities that can alter the decision making of an adversary but do not employ kinetic means. That is how we treat IO today—as the "other" operation. It is the drop-bucket for all the capabilities we have that do not involve the "real" work of the Army, putting firepower on a target. While many might object, it is impossible to dispute the fact that top Army officers earned their stars by starting their careers in, and staying connected to, the kinetic side of the house. The Army's information



U.S. Air Force, SA Nathanael Callon

U.S. Air Force 1LT Georganne Hassell, information operations officer with Provincial Reconstruction Team Zabul, helps Afghan students decorate scarves at the Zarghona Girls School in Qalat City, Zabul Province, Afghanistan, 8 July 2010.

warriors face a corporate culture challenge not unlike what the special operations forces community had to endure until Desert One in 1980 demonstrated the price of neglect.

Training: Achieving Acceptance through Relevance

The growing centrality of IO in Army doctrine owes its rise to the ongoing campaigns in Iraq and Afghanistan. Remote-controlled improvised explosive device attacks, hostile local civilians, Internet rumors, and other intangible scourges have frustrated the plans of too many commanders for too long. The real question is whether IO will survive our inevitable withdrawal from those two theaters.

After the wars in Iraq and Afghanistan conclude, it seems unlikely that the Army will discard IO as completely as it did PSYOP units in the immediate aftermath of Vietnam. It did so then in an effort to cleanse the stigma of that conflict, but today globalization has so tightly intertwined the movement of people, materiel, and information that the information environment is now the primary battlefield. This interconnectedness brings conflict. Those who feel they have suffered from globalization can now easily reach out and attack those who have benefited from it. Thus, information warriors will have to remain on call to defend our globally dispersed interests when the next conflict comes around, as it surely will.

To be of the greatest use to today's commanders and to avoid the same fate of the PSYOP units in the Army's post-Vietnam retooling, information warriors must prove their relevance to officers who will be tomorrow's generals.

I recommend a three-pronged approach to build the intellectual rigor and operational relevance of the information warrior: know your audience, know your tools, and know the machine.

- **Know your audience.** Articles in numerous journals have already gone into detail about the importance of language skills and cultural awareness to a contemporary ground force—and rightfully so, given the impact that deficiencies in these skills have had in ongoing operations. To their credit, the Marine Corps and Army have finally realized the value of providing cultural awareness and key-terms education for reducing the friction between patrols and local populations.

However, at the end of the day, the Army is not training the type of information warrior who can produce the strong cognitive impact that Hamas, Hezbollah, or Al-Qaeda propaganda teams do. The goal of any IO campaign is to influence a population—to alter the decisions they make—by shaping the information they absorb. Such a task is impossible if one does not understand the perceptual filters that affect that information absorption: language, individual bias, group dynamics, social pressures, and cultural norms. An information warrior should know the religious impact of every turn of phrase in the target audience's language, as well as the slang used and how to shape that language for age bracket, television, print media, or Internet outlets. Outsourcing message production to Madison Avenue types and the message management companies springing up all over the DC Beltway has yet to help a staff sergeant patrolling in Ar Ramadi or Lashkar Gah.

Nothing can replace the value of an information warrior with long-term language exposure gained through in-country cultural immersion. Ashley Jackson's recent article in *RUSI* journal points to numerous successes of British special forces during World Wars I and II in enemy rear areas.² These forces were commanded by officers and businessmen who had spent long portions of their lives in those theaters, the most successful and contemporarily relevant being the famous Lieutenant Colonel Thomas E. Lawrence (Lawrence of Arabia). And that is what the Army faces today—opposition forces who know what the local people need to hear and the threats, promises, or religious and tribal appeals that will get them to behave in particular ways.

Until information warriors are allowed to get inside a culture through long-term posting, something not currently compatible with the career track of a regular officer, this problem will persist. While the Defense Language Institute can give Soldiers understanding of a language, valuable on

...the information environment is now the primary battlefield.

standard patrols and interrogation, it is not enough to make them message masters. What they need is cultural immersion through cohabitation with a population. (Being a psychological operations team member on a forward operating base does not count.) The current operational environment does afford information warriors a chance to gain face-to-face exposure through provincial reconstruction teams and postings as an embedded advisor or instructor. These tours should be mandatory for any information warrior.

● **Know your tools.** The orchestration of an array of kinetic and nonkinetic capabilities in a dynamic human environment presents an information warrior with a complex set of operational choices. He must be a master of critical thinking and technical insight. The core skills of IO cover hard and soft (or social) sciences, with electronic warfare and computer network operations at one end of the spectrum and psychology operations, military deception, and operational security at the other. Both sides tend to attract a different personality type, and it is rare to find an individual who is a natural, ideal mixture of technician and philosopher. The purpose of melding electronic warfare, computer network operations,

psychological operations, military deception, and operations security was to create synergies of effect by their proper combination in the mission space as a kind of cognitive combined arms team. However, becoming proficient in one of these disciplines, let alone the various subdisciplines, requires years of training and field experience. (The electronic warfare community has been the most vocal about the hazards of the IO conglomeration. A frequent claim is that an information warrior is like a pool of water eight feet wide and one foot deep, while a good electronic warfare officer is one foot wide and eight feet deep.)

It may be impossible for an information warrior to be all things to all people, but it is possible to create one who is comfortable enough in each of the core capabilities to know when and how to use them to achieve mission objectives or recognize when he cannot. Comfort with all IO core capabilities is essential because it is a common human trait to follow the most comfortable course of action in moments of crisis and stress, rather than doing what is best. This is similar to the idea that “If all you have is a hammer, every problem is a nail.” While training can allow an individual



US Army. SGT Luis Delgadillo

COL James W. Adams, deputy commander of the 2d Brigade Combat Team, 3d Infantry Division, Fort Stewart, GA, listens to a sheik's concerns during a meeting at Forward Operating Base Kalsu, while SSG Shawn Wenninger, in charge of information operations, takes notes, 4 January 2010.

to achieve a high level of skill in performing a function under stress, the performance of the function can often lead to a loss of focus on why the function is necessary. A firm grounding in the fundamental knowledge of each core capability unified by an understanding of strategic theory and national strategy helps maintain a sense of focus when carrying out an IO campaign.

Comfort with each of the core capabilities will require frequent sabbaticals to universities or long-term specialty schools to learn and stay current on the various IO skill sets. Such sabbaticals can tie in with language and cultural immersion by studying or teaching at foreign universities or military technical schools. This has the natural result that an information warrior will be out of rotation longer than his peers are. Even so, at the end of the day, what is important is exposure to an interdisciplinary education so that he begins to think in increasingly creative ways to connect capabilities with mission objectives.

However, the information warrior cannot do it alone. He will have to rely on a cadre of technically trained warrant officers and noncommissioned officers to carry out the highly specialized tasks that make up the core capabilities. For example, it takes seven years to train a truly competent technical electronic intelligence specialist. This is not a progression conducive to an officer career, or one that lends itself to pursuing other training.

- **Know the machine.** An information warrior can instantly be of use to task forces, Joint force commanders, headquarters elements, and the like, if he has training in both the hard and soft sciences. However, unless he can get others in his command, especially the operations staff (S3, G3, J3), to understand how IO core capabilities fulfill mission objectives and to incorporate them into courses of action, then he might as well not have been trained at all.

...the information environment is now the primary battlefield.

Information operations are nonkinetic activities in the land of the kinetic. Units are full of officers who joined the Army to put firepower on a target, and received promotions based on their ability to do so. Information warriors are the odd ducks, like intelligence officers, who promise to add value to military activities, but the methods of their operation and their results seem almost imperceptible. (They lack the visual, psychological, and measurable impact of something blowing up.) The Army does not want units conducting IO just because it is required by DA to complete a certain number of IO activities quarterly. It wants its units to actually recognize the value of coordinating the “open hand” of IO with the “clenched fist” of kinetic operations. U.S. Strategic Command is still years away from developing munitions effectiveness for all of the IO capabilities, but even when they are incorporated into planning, without a strong information warrior, or previous IO training, these staffs will consistently default to what they know and are comfortable with. Humans will often go to the 70 percent solution they know rather than the 90 percent solution they do not.

This is the type of environment that every information warrior should be prepared to walk into. Many commanders who have repeatedly dealt with riotous populations (needing good psychological operations) or remote-controlled explosives (requiring electronic warfare) recognize the limits of the clenched fist. Even so, information warriors will still be pushing the new and the different—in essence, the disruptive.

An information warrior needs to be empathetic to the lifestyle and concerns of the Soldiers he works with. He needs to be able to talk shop with them and make them realize he knows what their world is like. Frequent cross-postings to other job billets, where IO is not the primary concern, has two advantages: it exposes the information warrior to how Soldiers work and choose courses of actions, and it brings a person who knows how to leverage IO into a unit that might not realize what IO can do. Platoon leaders in Afghanistan did not realize how indispensable National Geospatial Intelligence Agency imagery intelligence products were until the U.S. Air Force officer attached to their task force showed them their patrol route

before they moved out. That Air Force officer then became the most protected person in the unit. That is the type of impact an information warrior needs to aim for.

Moving Forward

An information warrior should be an interdisciplinary expert in the use of a variety of hard and soft science skills and know how those skills will impact the political, military, economic, social, informational, and infrastructural elements of a mission. He must understand the desired end state of his area of responsibility, the information environment and human terrain in that area, and how he can use IO to connect the two. The information

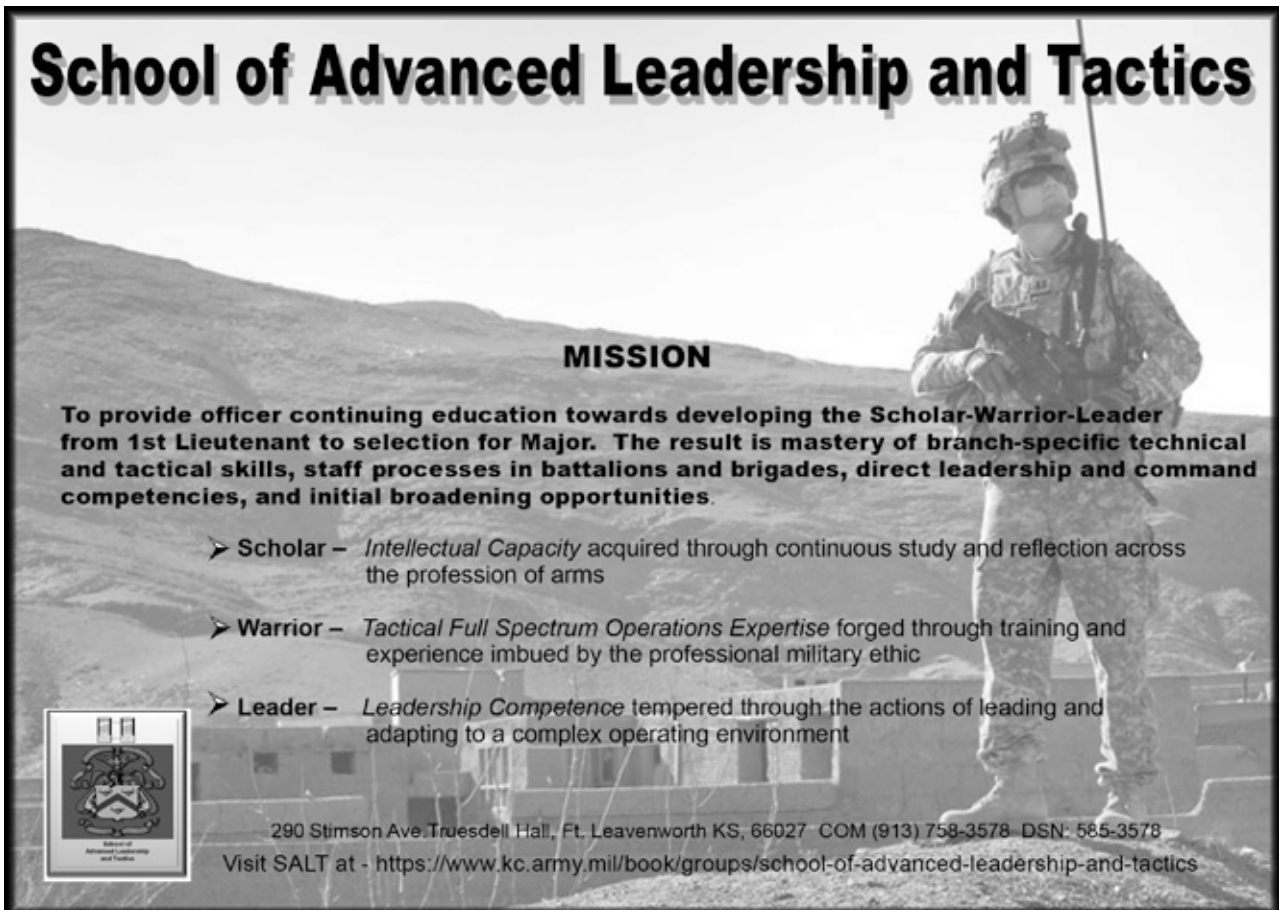
warrior is the pivot upon which the force's nonkinetic capabilities spin to complement the greater military strategy in the information environment.

Do not think that the Army can simply establish the IO career field, train a few officers, and consider itself ready to compete. The career field is only the first step in building a competitive advantage, the first, and long overdue step of an evolutionary shift in how the Army will deal with its missions in a globalized world. Just creating more information warriors and posting them in more places is not enough. We must develop a logical, rigorous, and comprehensive training strategy to make them relevant in their operational environment. **MR**

NOTES

1. United States Joint Publication 3-13, *Information Operations* (Washington, DC: Joint Chiefs of Staff, 2006).

2. Ashley Jackson, "The Imperial Antecedents to British Special Forces.," *RUSI Journal* 154, no. 3.




School of Advanced Leadership and Tactics

MISSION

To provide officer continuing education towards developing the Scholar-Warrior-Leader from 1st Lieutenant to selection for Major. The result is mastery of branch-specific technical and tactical skills, staff processes in battalions and brigades, direct leadership and command competencies, and initial broadening opportunities.

- **Scholar** – *Intellectual Capacity* acquired through continuous study and reflection across the profession of arms
- **Warrior** – *Tactical Full Spectrum Operations Expertise* forged through training and experience imbued by the professional military ethic
- **Leader** – *Leadership Competence* tempered through the actions of leading and adapting to a complex operating environment



290 Stimson Ave. Truesdell Hall, Ft. Leavenworth KS, 66027 COM (913) 758-3578 DSN: 585-3578
Visit SALT at - <https://www.kc.army.mil/book/groups/school-of-advanced-leadership-and-tactics>